REMARKS/ARGUMENTS

Claims 1-15 remain pending. No amendments have been made in this response.

Claim Objections

Claims 4 and 5 were objected to as being dependent upon a rejected base claim. The office action indicated that Claims 4 and 5 would be allowable if rewritten in independent form to include all the limitations of the base claim and any intervening claims.

Claims 4 and 5 depend from Claim 1, which is an allowable claim for the reasons set forth hereinbelow. Accordingly, Claims 4 and 5 are also allowable, and Assignee respectfully submits that this objection with respect to these claims is now moot.

Rejections Under 35 USC 102(e) Based on Aull

Claims 1-3, 6, 7, 12 and 14 were rejected under 35 USC §102(e) as being anticipated by U.S. Patent No. 7,028,180 to Aull (hereinafter "the '180 Patent").

Aull's '180 Patent discloses a method and computer program product for creating and using a role certificate in the encryption and signature of electronic documents. ('180 Patent, Abstract) Members of a group can then share the same role certificate and sign on behalf of the group. The '180 Patent further discloses that group members could also decrypt messages which have been sent to the group or any of its members, where the messages have been encrypted using the role certificate.

The '180 Patent discloses a process for creating a role certificate whereby a user accesses a registration web server and fills out an electronic form requesting a role certificate. ('180 Patent, Col. 9:7-10) The user signs the form and transmits it to the registration server. ('180 Patent, Col. 9:11-13) If the user is authorized to access the role certificate, then the role certificate is generated and sent to the user. ('180 Patent, Col. 9:22-50) A registration authority generates a new role certificate for encryption and signature that includes both a private and public key. *Id.*

Aull does not teach or suggest a limitation for calculating "a private key by means of parameters provided by the reliable authority and by parameters randomly selected by the person to be registered," as required by independent Claims 1, 12 and 14. By their dependence on Claim 1, Claims 3, 6 and 7 also include this limitation. Thus, the '180

Patent does not teach this limitation as it relates to any of the aforementioned rejected claims.

The '180 Patent discloses a process pursuant to which the user is permitted to sign an electronic form with the role certificate on behalf of an organization. ('180 Patent, Col. 9:51-10:3) However, the '180 Patent does not teach or suggest the limitation "defining a sequence including for the reliable authority generating a serial number to be used in the signing phase," as required by Claim 1. By their dependence, Claims 2, 3, 6 and 7 also require this limitation.

Moreover, the '180 Patent does not teach or suggest a signing phase during which a signature is issued specific to members of the list, "the signature being built so as to contain proof that the member of the list having issued the signature has a certificate of membership of the list," as required by independent Claims 1, 12 and 14. By their dependence, Claims 2, 3, 6 and 7 also require this limitation.

It should also be noted that, even if Aull teaches a group signature, Aull does not ensure that the signature is linkable as described in the present application at page 2, lines 2-10 and page 16 lines 10-31. In accordance with the present disclosure, one can determine whether two signatures were or were not issued by the same person without breaking the anonymity of the signature. Aull's '180 Patent does not consider this issue.

Nor does the'180 Patent teach or suggest the limitation for "a signature element which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number was used for generating the signature." This limitation is required by Claim 1, 12 and 14. By their dependence, Claims 2, 3, 6 and 7 also require this limitation.

The '180 Patent discloses a process for revoking a role certificate or role that is suspected of being compromised. ('180 Patent, Col. .11:33-11:62; Col. 12:25-12:39) However, the '180 Patent does not teach or suggest a revocation that "updates the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the member from the list." This limitation is required by Claim 1 and 12. By their dependence, this limitation is included in Claims 2, 3, 6 and 7.

Rejections Under 35 USC 102(e) Based on London Schrader

Claims 8-11, 13 and 15 were rejected under 35 USC §102(e) as being anticipated by U.S. Patent Publication 20020077887 to London Schrader et al. (hereinafter "the '887 Publication").

London Schrader discloses an architecture and method for anonymous electronic voting over a computer network. According to the London Schrader disclosure, voting is accomplished using a pair of public and private keys, and not a separate user identification and password for each election. [the '887 Publication, [0034])

Using the electronic voting system of the '887 Publication, a request for ballot is sent from a voting entity. ('887 Publication, Abstract) After the request is analyzed and validated, the ballot is sent to the voting entity. *Id.* The ballot includes unique election identification information and a serial number. ('887 Publication, [0061]) The ballot is encrypted with the public key of a voting tabulator and sent by a voting mediator to the voting entity. The voting entity receives the encrypted ballot and casts its votes. The voting entity also encrypts the votes and the encrypted ballot with the public key of the voting tabulator. This information is sent to the voting tabulator *without signature* due to the anonymous voting feature. ('887 Publication, [0062]) The encrypted ballot is sent from the voting tabulator to the voting mediator to ensure that the ballot was issued by the mediator and has not been previously used. After the mediator confirms the ballot, the voting tabulator increments the vote totals that correspond to the candidates chosen by the voting entity. ('887 Publication, [0063])

The '887 Publication does not teach or suggest "a phase of registering voters...during which each voter to be registered calculates a private key by means of parameters provided by the reliable authority and by parameters randomly selected by the voter to be registered," as required by independent Claim 8 of the present application. Because Claims 9-11 depend from Claim 8, the '887 Publication does not teach this limitation with respect to dependent Claims 9-11 as well. Similarly, as required by Claim 13, the '887 Publication does not teach "transmitting to each person to be registered in the list of voters parameters to be used for calculating a private key by means of parameters randomly selected by the person to be registered..." Also similarly, as required by Claim

15, the '887 Publication does not teach or suggest "receiving from a reliable authority parameters to be used for calculating a private key" and "calculating a private key by means of the received parameters and parameters randomly selected."

Moreover, as required by Claim 8, the '887 Publication does not teach "a phase of defining a sequence for the elections including, for the reliable authority, generating a serial number to be used in a voting phase..." Because Claims 9-11 depend from Claim 8, the '887 Publication does not teach or suggest these features with respect to these dependent claims as well. Similarly, with regard to independent Claim 13, the '887 Publication does not teach or suggest "generating a serial number specific to the poll, to be used by the members registered in said list of voters for generating an anonymous signature of a ballot specific to the members of the list of voters, this signature of a ballot being built so as to contain proof that the member of the list of voters having issued the signature, has a certificate of members of the list of voters..." Similarly, with regard to Claim 15, the '887 Publication does not teach or suggest "receiving a serial number to be used for generating an anonymous signature of a ballot for said poll..." In fact, the '887 Publication teaches away from ballot signatures: the '887 Publication explicitly discloses that the ballot is *not signed by the user* to ensure that the voting is anonymous.

Moreover, the '887 Publication does not teach or suggest a counting phase during which the ballots are verified, as recited by Claim 8.

The '887 Publication does not teach or suggest "a phase of revoking a member of a list of voters in order to remove a member from the list," as required by Claim 8. Similarly, as required by Claim 13, the '887 Publication does not teach or suggest "removing a member of the list of voters to be revoked, and updating the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the revoked member from the list of voters..."

Accordingly, the '887 Publication does not teach or suggest the limitations required by Claims 8-11, 13 and 15 of the present application. Assignee respectfully submits that these claims are patentable.

Conclusion

The undersigned respectfully submits that this application is in condition for allowance. Early and favorable reconsideration and allowance of this application is

respectfully requested. If any outstanding issues might be resolved by an interview or an Examiner's amendment, the Examiner is invited to call the representative of the assignee of the entire interest of this application at the telephone number shown below.

Because this office action is filed within three (3) months of the PTO mailing date, Assignee believes no fees are due at this time. However, if any petition for extension of time is deemed necessary, a petition under 37 C.F.R. 1.136 is hereby made.

Respectfully submitted,
BURTON IP LAW GROUP

Daphne L. Burton
Registration No. 45,323

2029 Century Park East
Suite 1400
Los Angeles, California 90067
Date: May 4, 2009
Direct dial: 310.867.2754
Facsimile: 310.867.2784